FINITE PHYLOGENETIC COMPLEXITY OF $\mathbb{Z}_p$ AND INVARIANTS FOR $\mathbb{Z}_3$

MATEUSZ MICHAŁEK

ABSTRACT. We study phylogenetic complexity of finite abelian groups - an invariant introduced by Sturmfels and Sullivant [SS05]. The invariant is hard to compute - so far it was only known for $\mathbb{Z}_2$, in which case it equals 2 [SS05, CP07]. We prove that phylogenetic complexity of any group $\mathbb{Z}_p$, where p is prime, is finite. We also show, as conjectured by Sturmfels and Sullivant, that the phylogenetic complexity of $\mathbb{Z}_3$ equals 3.

1. INTRODUCTION

The motivation for our work comes from phylogenetics - a science that aims at reconstructing the history of evolution. We will not present here all the concepts from phylogenetics as they are not needed for the statement and the solution of the problem that we study. Let us just say that to any tree T and a finite abelian group G, by considering a Markov process on a tree, one associates a projective toric variety $X(T, G)$. The explicit description of the variety and the associated polytope is given in Definition 2.2. We refer the interested reader to [PS05, ERSS04, SS05, Mic15, Mic11], where the relations to phylogenetics and applications are explained in detail. The equations defining $X(T, G)$ are called phylogenetic invariants. In all the cases that we study, determining phylogenetic invariants for any tree T was reduced to so-called star or claw trees using toric fiber product [SS05, Theorem 26], [Sul07, Corollary 2.11]. These trees, denoted by $K_{1,n}$ have one inner vertex and n leaves. Let us cite Draisma and Kuttler [DK09]:

"We have now reduced the ideals of our equivariant models to those for stars, and argued their relevance for statistical applications. The main missing ingredients for successful applications are equations for star models. These are very hard to come by (...)".

In our previous work with Maria Donten-Bury [DBM12] we have shown how to obtain phylogenetic invariants of bounded degree. However, it is highly nontrivial to obtain such a bound. To study these bounds Sturmfels and Sullivant defined two functions.

Definition 1.1 ($\psi(n, G), \psi(G)$)**.** *Let $\psi(n, G)$ be the degree in which the (saturated) ideal defining $X(K_{1,n}, G)$ is generated. Let $\psi(G)$, called the phylogenetic complexity of G, be the supremum of $\psi(n, G)$ over $n \in \mathbb{N}$.*

As observed by Sturmfels and Sullivant [SS05]: "The phylogenetic complexity $\psi(G)$ is an intrinsic invariant of the group G. (...) It would be interesting to study the group-theoretic meaning of this invariant." However, these invariants are very hard to compute. So far we only know $\phi(\mathbb{Z}_2) = 2$ [SS05, CP07]. Based on numerical computations Sturmfels and Sullivant proposed the following conjecture.

2010 *Mathematics Subject Classification.* Primary: 14M25 Secondary: 52B20, 13P25.

Key words and phrases. phylogenetic complexity; phylogenetic invariants; conjecture of Sturmfels and Sullivant; group-based model.

Supported by a grant Iuventus Plus of the Polish Ministry of Science, project 0301/IP3/2015/73.

Conjecture 1.2. [SS05, Conjecture 29] *For any finite abelian group G we have $\psi(G) \leq |G|$.*

However, for $G \neq \mathbb{Z}_2$ we do not know if $\psi(G)$ is finite. Our first main theorem is as follows.

Theorem 1.3. *For any prime number p the phylogenetic complexity of $\mathbb{Z}_p$ is finite.*

Depending how general the model is there are other qualitative results on the degree of phylogenetic invariants. For very general, so-called equivariant models, the fact that on set-theoretic level there exists a bound was proved in [DK09, DK14, DE15]. For the class of G-models that includes all the models introduced in this article, on the level of projective schemes the bounds were obtained in [Mic13]. Finally, for group-based models, but *only on Zariski open set,* the bound of the degrees by $|G|$ was proved in [CFSM14]. Our second main theorem is as follows.

Theorem 1.4. *The phylogenetic complexity of the group $\mathbb{Z}_3$ equals* 3.

This allows to find all phylogenetic invariants for any tree for the group $\mathbb{Z}_3$. As far as we know, this is the only model, different from the Jukes-Cantor model, where the complete list of phylogenetic invariants for any tree is obtained. For real data applications of phylogenetic invariants we refer for example to [RH12]. We would also like to mention that a related result was recently obtained by Donten-Bury in [DB16] on scheme-theoretic level.

The techniques that we use rely entirely on algebraic combinatorics. We present the above described problems in the combinatorial terms in Section 2. In different words, we study algebraic properties of a family of integral polytopes.

Although the original construction of varieties $X(T, G)$ was inspired by phylogenetics, recently they appeared in other sciences [Man09, Man12, Man13, SX10]. We would like also to mention that the varieties $X(T, G)$ share many other very interesting algebraic and combinatorial properties related to their Hilbert polynomial, normality and deformations [BBKM13, BW07, Kub12, MRV14].

The problems of the degrees in which toric ideals are generated appear in many different contexts [Bru13]. Let us summarize the results and conjectures about group-based models in the following table.

	Group-based Models				
polynomials defining:	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_p$	G
Gröbner basis	degree 2 by [CP07]				Question 1.5
generators of the ideal	degree 2 by [SS05]	degree 3 by Theorem 1.4	Conjecture [SS05, Conjecture 30]	finite by Theorem 1.3	Conjecture 1.2 [SS05, Conjecture 29]
the projective scheme		degree 3 [DB16]	degree 4 [Mic13]		finite by [Mic13]
set-theoretically					finite by [DE15]
on a Zariski open subset			degree 4 [Mic14]		degree $\leq |G|$ [CFSM14]

As one can see the higher the row, the finer algebraic properties are required. On the other hand columns to the right provide bigger and more general groups. This provides our table with "diagonal" structure with theorems mostly on and below the diagonal and conjectures above it. Taking this into account the following question, for now out of reach, is the most difficult.

Question 1.5. *What are the bounds on the degree of Gröbner basis for group-based models?*

Acknowledgements

The project was started when the author was visiting Freie Universität in Berlin thanks to Mobilność Plus program of the Polish Ministry of Science. The author is also a member of AGATES group and PRIME DAAD fellow. We would like to thank two reviewers for suggesting many improvements.

2. Definitions

Throughout the article G will be a finite abelian group. Let $[n] = \{1, \dots, n\}$.

Definition 2.1 (Flow)**.** *Fix $n \in \mathbb{N}$. A group-based flow f (on n) or simply a flow is a function $f : [n] \to G$ represented by an n-tuple of group elements $(f(1) = g_1, \dots, f(n) = g_n)$ and satisfying $\sum_{i=1}^{n} f(i) = 0 \in G$. With a coordinate-wise action flows form a group of flows $\mathcal{G}$ isomorphic to G^{n-1}.*

We will say that an element $g \in G$ belongs to a flow f if it belongs to the image of f. We let $\underline{0} = (0, \dots, 0)$ be the neutral element of $\mathcal{G}$.

The object of our study is a family of integral polytopes indexed by an integer $n \in \mathbb{N}$ and a finite abelian group G. These polytopes are combinatorial objects representing the group of flows $\mathcal{G}$. They are subpolytopes of a unit cube, hence all their integral points are vertices. The vertices are in bijection with elements of $\mathcal{G}$.

Definition 2.2 (Polytope $P_{n,G}$)**.** *Consider the lattice $M \cong \mathbb{Z}^{|G|}$ with a basis corresponding to elements of G. Consider M^n with the basis $e_{(i,g)}$ indexed by pairs $(i, g) \in [n] \times G$. We define an injective map of sets:*

$$\mathcal{G} \to M^n,$$

by $f \to \sum_{i=1}^{n} e_{(i,f(i))}$. The image of this map defines the vertices of the polytope $P_{n,G}$.

Example 2.3. *For $n = 3$ and $G = \mathbb{Z}_2$ we have four flows:*

$$(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Hence, the polytope $P_{3,\mathbb{Z}_2}$ has the following four vertices corresponding to the flows above:

$$(1, 0, 1, 0, 1, 0), (1, 0, 0, 1, 0, 1), (0, 1, 1, 0, 0, 1), (0, 1, 0, 1, 1, 0) \in \mathbb{Z}^2 \times \mathbb{Z}^2 \times \mathbb{Z}^2,$$

where $(1, 0) \in \mathbb{Z}^2$ corresponds to $0 \in \mathbb{Z}_2$ and $(0, 1) \in \mathbb{Z}^2$ corresponds to $1 \in \mathbb{Z}_2$.

The operation of addition is *different* for the two representations. Under the first representation flows form the finite group $\mathcal{G}$ – in particular, every element has finite order (equal to two in Example 2.3). Under the second representation the addition is simply addition of integer vectors induced from $\mathbb{Z}^{n|G|}$. In particular, every element has infinite order (and in Example 2.3 the four vertices are independent).

The polytope $P_{n,G}$ does not have to be normal (however for many groups it is conjectured to be). The associated toric variety in the sense of [Stu96] is isomorphic to $X(K_{1,n}, G)$ and is the main object of our study. However, as we will see, the language of flows, due to the group structure, is easier and will be used throughout the article instead of the language of polytopes and integral points. We refer the reader to [Ful93, CLS11] for background on toric varieties.

Phylogenetic invariants, that is equations defining $X(K_{1,n}, G)$, correspond to integral relations among vertices of $P_{n,G}$. We use the following combinatorial restatement. We say that two multisets of flows (on n) M_1 and M_2 are *compatible* if for any $i \in [n]$ we have $\cup_{f\in M_1}\{f(i)\} = \cup_{g\in M_2}\{g(i)\}$ as multisets of elements of G. This is equivalent to the fact that corresponding vertices sum up to the same lattice element. Of course to two compatible multisets we can add a flow, obtaining two bigger compatible multisets. The degree of a binomial corresponding to compatible multisets M_1, M_2 equals the cardinality of any of the multisets (note that both have to be of the same cardinality). By *exchanging* a multiset of group based flows we will always mean exchanging it with a compatible multiset.

Example 2.4. *For $G = \mathbb{Z}_2$ and $n = 6$ using the representation of flows as tuples of group elements we have e.g. the following two compatible multisets:*

$$M_1 = ((1, 1, 1, 1, 1, 1), (0, 0, 0, 0, 0, 0), (1, 1, 1, 1, 0, 0))$$

and

$$M_2 = ((0, 1, 0, 1, 0, 0), (1, 1, 1, 0, 1, 0), (1, 0, 1, 1, 0, 1)).$$

We could represent them as tables:

$$T_1 = \begin{matrix} (1,1,1,1,1,1) \\ (0,0,0,0,0,0) \\ (1,1,1,1,0,0) \end{matrix}$$

and

$$T_2 = \begin{matrix} (0,1,0,1,0,0) \\ (1,1,1,0,1,0) \\ (1,0,1,1,0,1) \end{matrix} .$$

Note that any *two flows from M_1 are* not compatible *with any two flows from M_2. However, $((1, 1, 1, 1, 1, 1), (0, 0, 0, 0, 0, 0))$ is compatible with $((0, 1, 0, 1, 0, 0), (1, 0, 1, 0, 1, 1))$, hence we may* exchange *them obtaining:*

$$\tilde{M}_1 = ((0, 1, 0, 1, 0, 0), (1, 0, 1, 0, 1, 1), (1, 1, 1, 1, 0, 0)).$$

Now M_1 and $\tilde{M}_1$ are compatible *and the last two flows in $\tilde{M}_1$ are compatible with the last two flows of M_2. Hence, we have a sequence of compatible multisets $M_1 \sim \tilde{M}_1 \sim M_2$.*

We started from a degree three binomial and generated it using degree two binomials.

The ideal of the variety $X(K_{1,n}, G)$ is generated in degree d if and only if the compatiblilty relation on multisets equals the transitive closure of the restriction of compatibility relation to multisets of cardinality at most d and the operation of adding a flow. More explicitly, if and only if we are able to pass from any multiset to any compatible multiset in a series of steps, each time exchanging a submultiset (of one multiset) with at most d flows by a compatible multiset of flows. By exchanging two flows f, g (in one multiset) on a set of indices I, we will mean replacing them with two flows f', g' such that $f'(i) = f(i)$ and $g'(i) = g(i)$ for $i \notin I$, $f'(i) = g(i)$ and $g'(i) = f(i)$ for $i \in I$. Notice that this is only possible if $\sum_{i\in I} f(i) = \sum_{i\in I} g(i)$.

Example 2.5. *Using the notation as in Example 2.4 while passing from M_1 to $\tilde{M}_1$ we exchanged $f = (1, 1, 1, 1, 1, 1)$ and $g = (0, 0, 0, 0, 0, 0)$ on indices $I = \{1, 3, 5, 6\}$ obtaining $f' = (0, 1, 0, 1, 0, 0)$ and $g' = (1, 0, 1, 0, 1, 1)$.*

3. Bounded phylogenetic complexity for $\mathbb{Z}_p$

We hope that the arguments of this section will be generalized to arbitrary finite abelian groups in future work. The whole section is devoted to the proof of Theorem 1.3. We will prove an equivalent statement: for n large enough, the ideal corresponding to the claw tree with $n+1$ leaves is generated in the same degree as for n leaves, that is $\psi(n+1, \mathbb{Z}_p) = \psi(n, \mathbb{Z}_p)$.

Consider two compatible multisets M_1 and M_2 of flows on $n+1$. The proof that one can pass from M_1 to M_2 exchanging at most $\psi(n, \mathbb{Z}_p)$ flows at each step is inductive on the cardinality of M_1 (that is the same as the cardinality of M_2). The case when M_1 is of cardinality one (or at most $\psi(n, \mathbb{Z}_p)$) is trivial.

Otherwise, choose $f_1 \in M_1$ and $g_1 \in M_2$. Suppose that f_1 and g_1 agree on k indices. In our proof we inductively increase k. If $k = n+1$ we can conclude (as $f_1 = g_1$) by reducing to the case of smaller cardinality of the multisets.

We distinguish two basic cases. Briefly, in the first one the flows f_1 and g_1 differ a lot, i.e. k is small. Here we can easily conclude using Lemma 3.1 that will also be useful in the following Section 4. In the second case we first consider the situation in which all the flows in M_1 and M_2 are very much alike. This is similar e.g. to the approach presented in [LM14]. The application of the results of [Mic13] allows us to finish the proof.

Lemma 3.1. *Fix $G = \mathbb{Z}_p$ for p a prime number. Suppose there exist two flows f, g and a set of indices I of cardinality $p-1$ such that for each $i \in I$ we have $f(i) \neq g(i)$. Then for any subset of indices I' disjoint from I there exists a subset $I'' \subseteq I$ such that we can exchange f and g on $I' \cup I''$.*

Proof. One possible proof, that we leave as an exercise for the reader, is by induction. We propose a different one based on Combinatorial Nullstellensatz [Alo99, Mic10, Las10].

Taking $-h := \sum_{i \in I'} f(i) - g(i)$, it is enough to show that there exists a subset $I'' \subset I$ such that $\sum_{i \in I''} f(i) - g(i) = h$. Let us consider the polynomial:

$$\prod_{h' \neq h} \left(\left(\sum_{i \in I} (f(i) - g(i)) x_i \right) - h' \right) \in \mathbb{Z}_p[x_i]$$

with nonzero coefficient of $\prod_{i \in I} x_i$. By Alon's Nullstellensatz there exists a point $P \in \{0,1\}^{|I|}$ on which the polynomial does not vanish. The coordinates of P which are nonzero identify a subset $I'' \subset I$ with the desired property. □

By the action of $\mathcal{G}$ (i.e. adding a fixed flow to all other flows) we may assume $g_1 = \underline{0}$. Let $I := \{i : f_1(i) \neq 0\}$. For each $i \in I$ there must exist a flow $f \in M_1$ such that $f(i) = 0$.

We first conclude in the easy case:

Case 1) $|I| > 3p^2$.

As all nonzero elements of G are indistinguishable, we may assume that there are $3p$ indices i, such that $f_1(i) = 1$. Let I' be the set of such indices. For any $j \in I'$ we may assume that any flow $f \in M_1$ such that $f(j) = 0$ has to assign one to all but at most $p-1$ indices from I', i.e. it has to agree with f_1 on I' on all apart from at most $p-1$ indices. Indeed, otherwise by Lemma 3.1, we can exchange f and f_1 on a subset of I' that contains j and increase k. Also other flows $f' \in M_1$ must assign 1 to at least $3p - 2p = p$ indices of I' as otherwise we would be able to exchange them first with an f such that $0 \in f(I')$ and then conclude as above. As M_1 and M_2 are compatible, there must exist a flow $g \in M_2$ that assigns one to at least p elements in I'. We can make an exchange between g and g_1 increasing k.

Hence, from now on we assume:

Case 2) $|I| \leq 3p^2$.

Our aim is to reduce to the situation, in which there exists one flow $f_0 \in M_1$ such that $f_0(i) = 0$ for all $i \in I$ (or similarly a flow $g_0 \in M_2$ such that $g_0(i) = f_1(i)$ for all $i \in I$). This will finish the proof, as then we can exchange f_1 and f_0 on I (recall that f_1 is a flow and $f_1(s) = 0$ for $s \notin I$). Hence, we fix a flow f_0. Our strategy in this case is to apply results of [Mic13] to prove the main Lemma 3.5. Once it is proved, one can easily increase $|\{i \in I : f_0(i) = 0\}|$. It is often useful to encode flows as colorings.

Definition 3.2 (Coloring)**.** *A coloring of length n is a function $f : [n] \to [g] \cup \{0\}$. The number g is called the number of colors. The support of the coloring f is defined as $\{k \in [n] : f(k) \neq 0\}$.*

Definition 3.3 (Transformation)**.** *Consider two colorings $f_1, f_2 : [n] \to [g] \cup \{0\}$. Suppose that there exist two numbers $0 \leq k_1, k_2 \leq n$ such that k_j is* not *in the support of f_j. Moreover suppose $f_1(k_2) = f_2(k_1)$. Define $f'_j(x) = f_j(x)$ for $x \neq k_1, k_2$. Moreover, $f'_1(k_j) := f_2(k_j)$ and $f'_2(k_j) := f_1(k_j)$. We call f'_1, f'_2 a* transformation *of f_1 and f_2.*

Transformation of colorings corresponds to exchanging the fixed color in two colorings with the 0 color. A multiset of colorings can be transformed into another by choosing two colorings and transforming them. We generate an equivalence relation on multisets of colorings by transformations. Abusing the notation the relation is also called transformation. We note that transformations of colorings give rise to compatible exchanges of multisets of flows (generated by quadrics).

Lemma 3.4. [Mic13, Lemma 6.5] *Let us fix three natural numbers: g (number of colors), s (bound on the support) and $a \geq 2$. Fix $\epsilon > 0$. There exists $N \in \mathbb{N}$, such that for all $n \geq N$ any collection of colorings $f_1, \dots, f_m : [n] \to [g] \cup \{0\}$ with support of cardinality at most s can be transformed into a collection $f'_1, \dots, f'_m$ with the following property:*

there exist $\lfloor (1-\epsilon)\frac{n}{a} \rfloor$ numbers $x < n$ divisible by a, such that for any f'_j and any x at most one of the numbers $x, x+1, \dots, x+a-1$ is in the support of f'_j.

Lemma 3.5. *We may assume that there exist two flows $f_3, f_4 \in M_1$ different from f_1, such that $|j \notin I : f_3(j) \neq f_4(j)| > 2p$.*

Proof. Let us assume the contrary. By exchanging M_1 and M_2 we may assume that after restricting all flows to the complement of I:

(i) any two flows f_i, f_j different from f_1 differ on at most $2p$ indices,
(ii) any two flows g_i, g_j different from g_1 differ on at most $2p$ indices.

We will show that in this case we can transform M_1 to M_2 exchanging at most $\phi(n, G)$ flows at a time. We proceed in the following steps:

1) Show that there exists a function $q : [n+1] \setminus I \to G$ such that each flow $f \in M_1 \setminus f_1$ *and* each flow $g \in M_2 \setminus g_1$ differ from q (on the complement of I) on at most $4p$ indices.
2) Apply Lemma 3.4, to obtain two indices i_0, i_1, such that each flow $f \in M_1 \setminus f_1$ *and* each flow $g \in M_2 \setminus g_1$ differ from q on i_0, i_1 on at most 1 index.
3) Reduce to the case of flows on n.
4) Apply induction by lifting the exchanges among flows on n and generate the relation among flows on $n+1$.

Step 1:

Let q be the restriction of any flow in $M_1 \setminus f_1$ to the complement of I. By assumption (i) any other flow in $M_1 \setminus f_1$ differs from q on at most $2p < 4p$ indices. We want to show that also the flows in $M_2 \setminus g_1$ cannot differ from q on more than $4p$ indices.

We act (coordinate-wise) on $M_1 \setminus f_1$ with the inverse of the flow that defined q and restrict to the complement of I. Identifying $0 \in G$ with $0 \in \mathbb{N}$ and other group elements with consecutive natural numbers we obtain a multiset of colorings with the support bounded by $2p$. It remains to show that after this action also the elements of $M_2 \setminus g_1$ must have a bounded support. Indeed, on average every element of $M_2 \setminus g_1$ must have at most $2p$ nonzero elements (notice that after restricting to the complement of I the multiset $M_1 \setminus f_1$ is compatible with $M_1 \setminus g_1$). However, as the flows differ on at most $2p$ indices all flows must have at most $4p$ nonzero elements.

Step 2:

Taking $s = 4p$, $a = 2$, $\epsilon < 1/2$ and applying Lemma 3.4 to flows/colorings from $M_1 \setminus f_1$ and $M_2 \setminus g_1$ restricted to the complement of I we may assume that there exist:

(i) indices $i_0, i_1 \notin I$,
(ii) two group elements $g := q(i_0), h := q(i_1)$,

such that

(i) any flow f_j for $j \neq 1$ satisfies $f_j(i_0) = g$ or $f_j(i_1) = h$,
(ii) any flow g_j for $j \neq 1$ satisfies $g_j(i_0) = g$ or $g_j(i_1) = h$.

Step 3:

By permuting columns, for simplicity of notation assume $i_1 = i_0 + 1$. We may replace the flows f_j, g_j by flows f'_j, g'_j on n where:

$$f'_j(k) = \begin{cases} f_j(k) & k < i_0 \\ f_j(k+1) & k > i_0 \end{cases} \quad , f'_j(i_0) = f_j(i_0) + f_j(i_1)$$

$$g'_j(k) = \begin{cases} g_j(k) & k < i_0 \\ g_j(k+1) & k > i_0 \end{cases} \quad , g'_j(i_0) = g_j(i_0) + g_j(i_1).$$

The obtained multisets remain *compatible*. Indeed, restricting the flows to indices i_0, i_1 we obtain exactly the same pairs of group elements for M_1 and M_2 (these pairs are either (g, h) or (g, h') for $h' \neq h$ or (g', h) for $g' \neq g$).

Step 4:

By induction, for flows on n we only need to exchange at most $\phi(n, G)$ flows at each step. Notice, that each exchange lifts to an exchange among M_1 and M_2. Indeed, the exchanges on the summed entries lift to exchanges among pairs of indices i_0, i_1. Notice that this is *not* enough to conclude, as at the end we do not obtain the same multisets - just the multisets that after summing up entries i_0 and i_1 are the same. However, the entries on i_0 and i_1 may be adjusted using simple quadratic moves (i.e. exchanges among two flows), which finishes the proof of the lemma. □

We may now increase the number of indices $i \in I$ such that $f_0(i) = 0$. Choose $i_0 \in I$ such that $f_0(i_0) \neq 0$ and $f' \in M_1$ such that $f'(i_0) = 0$. Exchanging f_0 either with f_3 or f_4 from the lemma we may assume that f_0 and f' differ on at least $p - 1$ indices not from I. By Lemma 3.1 we can exchange f_0 and f' on index i and some indices not in I. This finishes the proof of Theorem 1.3.

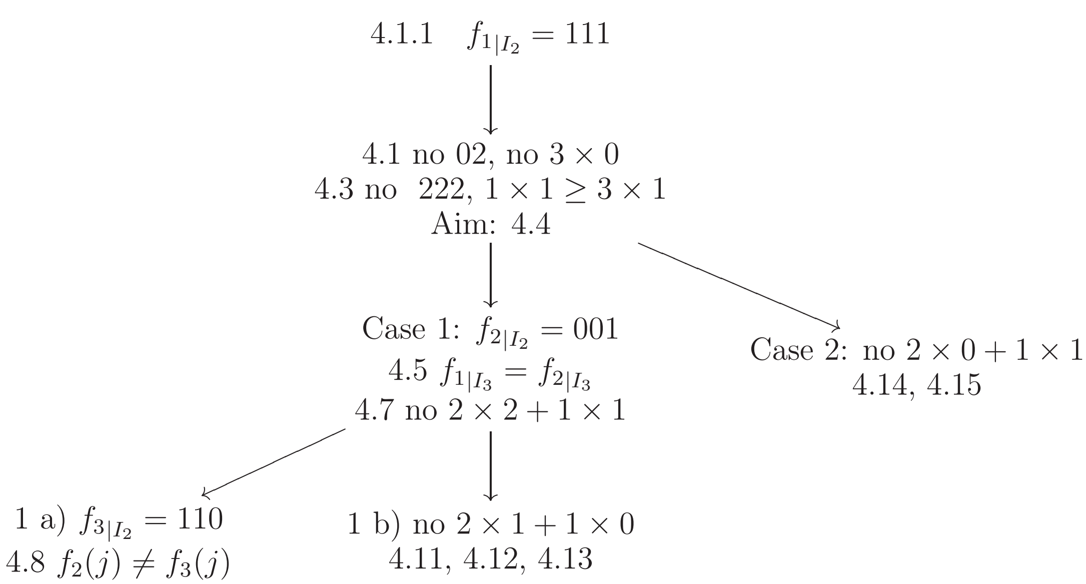
4. The phylogenetic complexity of $\mathbb{Z}_3$

The whole section is devoted to the (very technical) proof of Theorem 1.4. The main methods are as follows. For small n we use direct computational results using [BTRS01, tt, DBM12]. For large n the basic distinction into the case where two flows are very different or very much alike remains valid. However, in both cases (especially when two flows are much alike) we failed to find short, easy proofs or conclude simply by deeper and deeper case study. Our arguments rely on a mixture of counting arguments and combinatorial tricks. In particular, we believe that it is impossible to follow this proof without a pen and a sheet of paper. The author would much appreciate an approach that would be significantly simpler (as this would rise hope for attacking larger groups, e.g. [SS05, Conjecture 30]).

Our proof is inductive on n, the length of the flows. For fixed n we show inductively that any binomial of degree $d > 3$ is generated by cubics. For $n < 7$ it was known before that the ideal of $\mathbb{Z}_3$ is generated by cubics [DBM12]. Thus we assume $n \geq 7$. Let us fix two compatible multisets of group-based flows $M_1 = \{f_1, \dots, f_d\}$ and $M_2 = \{g_1, \dots, g_d\}$. To simplify the notation, by the action of $\mathcal{G}$ we may assume that $g_1 = \underline{0}$ is the trivial flow. Suppose that f_1 and g_1 agree on $k-1$ indices. Our aim is to increase k, until $k-1 = n$. Of course if $k-1 = n$ then $g_1 = f_1$ and we may conclude by the induction on d. By the action of the symmetric group S_n we may assume that $f_1(i) = 0$ if and only if $1 \leq i \leq k-1$. As the proof is quite complicated we decided to include diagrams that describes most important cases. While reading the proof we encourage the reader to follow at which node we are. The proofs are "depth-first, left-first".

4.1. **Suppose $k \neq n-1$.** There are two possibilities we consider. Either f_1 attains the same element for at least three indices greater or equal to k or $k = n-3$ and we can assume $f_1(k) = f_1(k+1) = 1$, $f_1(k+2) = f_1(k+3) = 2$.

4.1.1. *Suppose (by the action of the nontrivial automorphism of $\mathbb{Z}_3$) we have:* $f_1(k) = f_1(k+1) = f_1(k+2) = 1$. The diagram for this subsection is presented below. In each vertex we presented main case assumptions and lemmas with very short comments that the reader may unravel while following the proof.



Let us group the indices:

$$I_1 := \{1, \dots, k-1\}, I_2 := \{k, k+1, k+2\}, I_3 := \{k+3, \dots, n\}.$$

Note that I_1 or I_3 may be empty.

Lemma 4.1. *If there exists a flow $f \in M_1$ that has either*

(i) both 0 and 2 or
(ii) only 0,

in the image of I_2, then we can increase k.

Proof. In the first case, we may exchange the elements on the preimages of 0 and 2 in I_2 between f and f_1, increasing the number of neutral elements in f_1. In the second case we exchange f and f_1 on I_2. □

Remark 4.2. *As g_1 has only neutral elements in the image of I_2, for each $i \in I_2$ there must exist a flow $f \in M_1$, such that $f(i) = 0$. By Lemma 4.1 such flows f can be only of two types; either they have precisely twice 1 and once 0 in the image of I_2 or twice 0 and once 1.*

Lemma 4.3. *We may assume that:*

(i) there is no flow among M_1 that associates three times 2 on I_2,
(ii) there exist at least as many flows in M_1 that associate to I_2 exactly one 1 as those that associate three times 1.

Proof. Suppose that $f \in M_1$ associates three times 2 on I_2. There exists a flow $f' \in M_1$ that associates either twice 1 and once 0 or twice 0 and once 1 on I_2. We can make an exchange between f and f' on two indices from I_2 on which f' has value 0 and 1. This proves the first part of the lemma by Lemma 4.1.

Hence, also by Lemma 4.1 we see that each flow in M_1 has at least one 1 on I_2. If there are strictly more flows that associate three times 1 than those that associate 1 only once (with each of the other two entries equal either to 0 or 2), then an average of associations of 1 on I_2 for the whole M_1 is above 2. As M_1 and M_2 are compatible the same must be true for M_2. Hence, there must exist $g \in M_2$ that associates to I_2 three times 1. We can make an exchange between g and g_1 on I_2, increasing k by three. □

Our aim is to prove the following proposition.

Proposition 4.4. *We can compatibly change M_1, so that there exists a function $h : I_1 \cup I_3 \to \mathbb{Z}_3$ such that:*

(i) for every index $j_0 \in I_3$ we have $h(j_0) = f_1(j_0)$,
(ii) for any $f \in M_1 \setminus f_1$ there exists at most one index $j_0 \in I_1 \cup I_3$ such that $h(j_0) \neq f(j_0)$,

as otherwise we are able to increase k.

The proof of the above crucial proposition is divided into several parts.

Case 1) There exists a flow in M_1, say f_2, that in the image of I_2 has precisely two 0 and one 1. By the action of $S_{I_2} \subset S_n$ we may assume $f_2(k) = f_2(k+1) = 0$ and $f_2(k+2) = 1$. In this case the function h in Proposition 4.4 will be the restriction of f_2 to $I_1 \cup I_3$.

Lemma 4.5. *For any $i \in I_3$ we can assume $f_1(i) = f_2(i)$. For any $i \in I_1$ we have either $f_2(i) = 0$ or $f_2(i) = 1$. The number of $i \in I_1$ such that $f_2(i) = 1$ equals 2 modulo 3.*

Proof. Suppose there is $i \in I_3$ such that $f_1(i) \neq f_2(i)$. We may exchange f_1 and f_2 on i and on one or two indices $k, k+1$, so that we get two flows. This would increase k.

If there is $i \in I_1$ such that $f_2(i) = 2$ then we can exchange f_1 and f_2 on $i, k, k+1$. This would also increase k. The last statement follows from the first, because f_2 is a flow. □

Corollary 4.6. *Point 1) of Proposition 4.4 holds.* □

By Remark 4.2 there must exist a flow in M_1, say f_3, such that $f_3(k+2) = 0$.

Lemma 4.7. *We may assume that there are no flows in M_1 that to I_2 associate twice* 2 *and once* 1. *In particular, by Lemma 4.1, all flows that associate only one* 1 *on I_2 associate exactly two* 0.

Proof. Suppose such a flow f exists. We may assume that $f(k) = f(k+1) = 2$ and $f(k+2) = 1$ as otherwise we could conclude by Lemma 4.1, by exchanging f and f_2 on k, $k+1$. As above we must have $f_3(k) = f_3(k+1) = 1$. Exchanging f_3 and f_2 on $k+1$ and $k+2$ and then exchanging f with f_2 on k and $k+2$ we can conclude by Lemma 4.1. □

By Remark 4.2 we may consider the following two cases.

Case 1 a) $f_3(k) = f_3(k+1) = 1$.

Lemma 4.8. *On $I_1 \cup I_3$ any two flows f_{i_1} and f_{i_2} such that $\sum_{i \in I_2} f_{i_1}(i) = 1$ (e.g. f_2) and $\sum_{i \in I_2} f_{i_2}(i) = 2$ (e.g. f_3) differ on $I_1 \cup I_3$ on precisely one index j for which $f_{i_1}(j) = f_{i_2}(j) - 2$.*

Proof. By making exchanges with f_2 and f_3 it is enough to prove the lemma for these two flows. Suppose there exists an index $i \in I_1 \cup I_3$ such that $f_2(i) = f_3(i) + 2$. We may then exchange the flows f_2 and f_3 on the indices i and $k+2$. We obtain a flow that associates 0 to all the indices of I_2, which allows to increase k by Lemma 4.1.

Suppose there is more than one index $j_1, j_2 \in I_1 \cup I_3$ such that $f_2(j_i) = f_3(j_i) + 1$ for $i = 1, 2$. Then, as above, we may exchange f_2 and f_3 on j_1, j_2 and $k+2$. This finishes the proof - one such index must exist as f_2 and f_3 are flows. □

Definition 4.9 (index j)**.** *We define the distinguished index j to be the unique $j \in I_1 \cup I_3$ such that $f_2(j) \neq f_3(j)$.*

We now prove point 2) of Proposition 4.4. Consider any flow $f \in M_1$ different from f_1, f_2, f_3.

If $\sum_{i=k}^{k+2} f(i) = 2$ then by Lemma 4.8 we see that f differs from f_2 on $I_1 \cup I_3$ on precisely one index, that allows to conclude in this subcase.

If $\sum_{i=k}^{k+2} f(i) = 1$ we may exchange f and f_2 on I_2. By Lemma 4.8 we see that f differs from f_3 on $I_1 \cup I_3$ on precisely one index. As f_2 and f_3 agree on $I_1 \cup I_3 \setminus \{j\}$, we have two possibilities. Either f agrees with f_2 on $I_1 \cup I_3$ or there exists $j' \in I_1 \cup I_3 \setminus \{j\}$ such that $f(j) = f_2(j) + 2$ and $f(j') = f_2(j') - 2$. We have to exclude the latter case. By Lemma 4.1 we have $f(I_2) = \{1, 1, 2\}$ or $f(I_2) = \{0, 0, 1\}$. By the S_{I_2} action it is enough to consider the following.

If $f(k) = 2$ and $f(k+1) = f(k+2) = 1$ we exchange f and f_2 on j', k and conclude by Lemma 4.1. If $f(k+2) = 2$ and $f(k+1) = f(k) = 1$ we exchange f and f_2 on $j', k, k+1$. If $f(k) = f(k+2) = 0$ and $f(k+1) = 1$, we exchange f and f_2 on $j', k+2$ and also conclude by Lemma 4.1. If $f(k) = f(k+1) = 0$ and $f(k+2) = 1$ we can exchange f and f_3 on j', k and then f_2 and f_3 on $k+2, j'$. We obtain the following stronger statement.

Corollary 4.10. *All flows $f \in M_1$ such that $\sum_{i=k}^{k+2} f(i) = 1$ agree on $I_1 \cup I_3$.* □

To finish the proof we have to consider flows $f \in M_1 \setminus f_1$ for which $\sum_{i=k}^{k+2} f(i) = 0$. By Lemma 4.1 and Lemma 4.3 we have $f(k) = f(k+1) = f(k+2) = 1$.

Now, our strategy is a little different. We do not show directly that each f differs from h on one index. Instead, by Lemma 4.3 we associate to each such f a flow $\tilde{f}$ that associates only one 1 to I_2. We will show how to modify each pair, so that both flows differ from h on at most one index. By Lemma 4.7 we can further assume that $\tilde{f}(I_2) = \{0, 0, 1\}$. By Corollary 4.10 we know that $\tilde{f}$ agrees with h on $I_1 \cup I_3$. If f differs from $\tilde{f}$ on at least two indices from $I_1 \cup I_3$, we can exchange f and $\tilde{f}$ on precisely on index $i \in I_2$ such that $\tilde{f}(i) = 0$ and one or two indices from $I_1 \cup I_3$ reducing to previous cases when $\sum_{i=k}^{k+2} f(i) \neq 0$. This finishes the proof of Proposition 4.4 in Case 1 a).

Case 1 b) There is no flow in M_1 that associates 0 to $k+2$ and 1 to k and $k+1$. In particular, we may assume $f_3(k) = 0$ and $f_3(k+1) = 1$.

Lemma 4.11. *We can assume that all $f \in M_1$ such that $\sum_{i \in I_2} f(i) = 1$ agree on $I_1 \cup I_3$.*

Proof. It is enough to prove that f_2 and f_3 agree. Suppose $f_2(i) \neq f_3(i)$. Exchanging f_2 and f_3 we may assume that $f_2(i) = f_3(i) + 1$. Exchanging f_2 and f_3 on $i, k+2$ we conclude by Lemma 4.1. □

Lemma 4.12. *We can assume that all flows $f \in M_1$ such that $\sum_{i \in I_2} f(i) = 0$ agree with h on $I_1 \cup I_3$, apart from one index.*

Proof. By Lemmas 4.1 and 4.3 we have $f(I_2) = \{1, 1, 1\}$. Suppose $f(i) \neq f_2(i)$ for $i \in I_1 \cup I_3$. If $f(i) = f_2(i) + 1$ we can exchange f and f_2 on $k, k+1, i$ and conclude that i is the unique index with $f(i) \neq f_2(i)$ by Lemma 4.11. Suppose $f(i) = f_2(i) + 2$. Exchanging f and f_3 on $k+2, i$ reduces to Case 1 a). □

Lemma 4.13. *We can assume that all flows $f \in M_1$ such that $\sum_{i \in I_2} f(i) = 2$ agree with h on $I_1 \cup I_3$ apart from one index.*

Proof. By Lemma 4.1 the image $f(I_2)$ as a multiset must equal $\{0, 1, 1\}$ or $\{1, 2, 2\}$. Suppose it is $\{1, 2, 2\}$. There is a two element subset $B \subset I_2$ such that $f(B) = \{1, 2\}$ and either $f_2(B) = \{0, 0\}$ or $f_3(B) = \{0, 0\}$. We can exchange f and either f_2 or f_3 on B, obtaining a reduction by Lemma 4.1. Thus we assume $f(I_2) = \{0, 1, 1\}$. By Case 1 a) we can assume $f(k) = 0$ and $f(k+1) = f(k+2) = 1$. Let $i \in I_1 \cup I_3$ be such that $f(i) \neq f_2(i)$. If $f(i) = f_2(i) + 2$ we can exchange f and f_2 on $i, k+1$ obtaining the uniqueness of i by Lemma 4.11 (as after the exchange the flow must exactly agree with h on $I_1 \cup I_3$). Thus we assume $f(i) = f_2(i) + 1$. If $f_1(i) \neq 0$ we may exchange f and f_1 on i, k increasing k. Thus we assume $f_1(i) = 0$. There must exist one more index $j \in I_1 \cup I_3$ such that $f(j) = f_2(j) + 1$. By exchanging f and f_2 on $k+1, i, j$ by Lemma 4.11 we see that f agrees with f_2 on $I_1 \cup I_3 \setminus \{i, j\}$. As before $f_1(j) = 0$.

By Lemma 4.5 we assume that either $f_2(i) = 0$ or $f_2(i) = 1$. In the latter case $f(i) = 2$. We can apply the cubic relation among f_1, f_2, f that on indices $i, k, k+1$ is given by:

$$\begin{matrix} (0,1,1) & & (2,0,0) \\ (1,0,0) & = & (0,0,1) \\ (2,0,1) & & (1,1,1) \end{matrix}$$

and all other indices remain unchanged. This cubic relation increases k.

Hence, we may assume $f_2(i) = f_2(j) = 0$. Note that there must exist further indices $i', j' \in I_1$ such that $f_2(i') = f_2(j') = 1$. It follows that $f(i') = f(j') = 1$.

Claim: In the situation above, we can assume that each flow in M_1 different from f_1 attains at least three times 1 on indices $k+1, k+2, i'j'$.

Proof of the Claim. Consider any flow $f' \in M_1$ different from f_1.

Suppose $f'(k+1) = f'(k+2) = 1$. We have already shown that either f' differs from f_2 on $I_1 \cup I_3$ on one index, in which case the claim holds, or it disagrees on two indices, none of them equal to i', j', in which case the claim also holds.

Suppose $f'(k+1), f'(k+2) \neq 1$. By Lemma 4.1 it either associates twice 0 or twice 2. In the latter case we can exchange f' and f_2 on $k+1, k+2$ obtaining a contradiction with Lemma 4.1. In the former case, by the same lemma $f'(k) = 1$. This gives reduction to Case 1 a).

We are left with the case in which we can assume $f'(k+2) = 1 \neq f'(k+1)$. We consider two cases.

(i) $f'(k+1) = 2$. We have $f'(k) \neq 0$ by Lemma 4.1. If $f'(k) = 2$ then we can exchange f' and f_3 on $k, k+1$ obtaining contradiction with Lemma 4.1. Hence, $f'(k) = 1$. The Claim follows by Lemma 4.11.

(ii) $f'(k+1) = 0$. If $f'(k) = 0$ the Claim follows by Lemma 4.11. By Lemma 4.1 we can assume $f'(k) = 1$. This gives a reduction to Case 1 a).

This finishes the proof of the claim. □

Hence, f_1 is the only flow that can attain less than three times 1 on $k+1, k+2, i', j'$. However, f associates only 1 to all four indices. Hence, by the Claim the average over all flows in M_1 of 1 on these four indices is at least three. As $g_1 \in M_2$ does not have any 1 on these indices in follows that there must exist a flow $g \in M_2$ that associates 1 to all four indices. We can exchange g and g_1 on $k+1, k+2, i'$ which increases k. This finishes the proof. □

The Lemmas 4.11, 4.12, 4.13 finish the proof of Proposition 4.4 in Case 1b).

Case 2) None of the flows in M_1 associates twice 0 and once 1 on I_2. By the case assumption and Lemma 4.1 we can assume that:

$$f_2(k) = 0, f_2(k+1) = 1, f_2(k+2) = 1,$$
$$f_3(k) = 1, f_3(k+1) = 0, f_3(k+2) = 1,$$
$$f_4(k) = 1, f_4(k+1) = 1, f_4(k+2) = 0.$$

Lemma 4.14. *We can assume that the image of I_2 by any flow $f \in M_1$ as a multiset is equal to one of:*

$$\{1,1,1\}, \{1,1,0\}, \{1,1,2\}, \{1,2,2\}.$$

Proof. By Lemma 4.1 the only possible multiset that does not contain 1 is $\{2,2,2\}$, which is excluded by Lemma 4.3. If $f(I_2)$ contains exactly one 1, then by Lemma 4.1 it equals either $\{1,2,2\}$ or $\{1,0,0\}$, the latter possibility contradicting Case assumption. The other possibilities appear in the statement. □

We will now obtain a contradiction (which proves that we can always reduce to one of the previous cases or increase k). In analogy to Lemma 4.1, all flows $g \in M_2$ that do not contain 0 in the image $g(I_2)$ must attain three times 2 on I_2. To each such flow we can associate a flow $f \in M_1$ such that $f(k+2) = 2$. By Lemma 4.14 all such flows also do not have 0 in the image of I_2. Then we can pair arbitrarily other flows $g \in M_2$, $g \neq g_1$ with

flows $f \in M_1$, $f \neq f_1$. By Lemma 4.14 in each pair (f, g) the flow g attains 0 on I_2 at least as many times as f. Pairing g_1 with f_1, we obtain a contradiction with compatibility of M_1 and M_2 counting the number of 0 on I_2.

This finishes the proof of Proposition 4.4. The proposition assures the existence of a function h for M_1 and similarly h' for M_2. Notice that on $I_1 \cup I_3$ the functions h and h' can disagree only on at most 2 indices, as otherwise, just by comparing the indices on which the functions differ, we would have a contradiction with the fact that M_1 and M_2 are in a relation. Hence, for $n \geq 7$ we can find two indices $i, j \in I_1 \cup I_3$ on which h and h' agree.

Lemma 4.15. *For i, j as above the two multisets of pairs:*

$$\{(f(i), f(j)) : f \in M_1\}, \{(g(i), g(j)) : g \in M_2\}$$

are equal.

Proof. By definition the following multisets are equal:

$$\{f(i) : f \in M_1\} = \{g(i) : g \in M_2\}.$$

If in any of the two multisets an element o different from $h(i)$ appears it gives a pair $(o, h(j))$ in both of the multisets in the statement of the lemma. In the same way we have:

$$\{f(j) : f \in M_1\} = \{g(j) : g \in M_2\}$$

and each element $o' \neq h(j)$ gives a pair $(h(i), o')$. All the other pairs equal $(h(i), h(j))$. □

By Lemma 4.15 we can sum up entries on indices i, j obtaining two compatible multisets M_1', M_2' of flows of size $n-1$. By induction, such relation can be generated and we can lift each quadric and cubic in the generation process. After this procedure, it is enough to apply quadric relations, exchanging only flows on indices i, j to generate the relation represented by M_1, M_2. This finishes the case when f_1 attains three times an element different from 0.

4.1.2. *Let us now assume $k = n-3$, $f_1(k) = f_1(k+1) = 1$, $f_1(k+2) = f_1(k+3) = 2$.*

Lemma 4.16. *We can assume that there is no flow $f' \in M_1$ or $g' \in M_2$ such that:*

- *(i) ($f'(k) = 2$ and $f'(k+1) = 0$) or ($f'(k) = 0$ and $f'(k+1) = 2$) or ($f'(k+2) = 0$ and $f'(k+3) = 1$) or ($f'(k+2) = 1$ and $f'(k+3) = 0$) or ($f'(i) = 0$ and $f'(j) = 0$ for $i = k$ or $k+1$ and $j = k+2$ or $k+3$),*
- *(ii) ($g'(i) = 1$ and $g'(j) = 2$) where $k \leq i, j$ and either $i = k, k+1$ or $j = k+2, k+3$.*

Proof. As all the statements are similar and easy let us only prove the case $f'(k) = 2$ and $f'(k+1) = 0$. Then, we can exchange f' and f_1 on $k, k+1$. □

By symmetry we consider two cases.

Case 1) There exists a flow $f_2 \in M_1$ such that $f_2(k) = f_2(k+1) = 0$.

Lemma 4.17. *We may assume $f_2(k+2) = f_2(k+3) = 2$.*

Proof. Otherwise we could exchange f_1 and f_2 and increase k. □

Lemma 4.18. *We can assume that for any flow $f' \in M_1$ such that $f'(k+2) = 0$ (resp. $f'(k+3) = 0$) we have $f'(k) = f'(k+1) = 1$.*

Proof. By Lemma 4.16 for $i = k, k+1$ we have $f'(i) = 1$ or $f'(i) = 2$. If $f'(i) = 2$ we can exchange f' and f_2 on $i, k+2$ (resp. $k+3$) and conclude by Lemma 4.16. □

Hence, the flows in M_1 associate strictly more times 1 on indices $k, k+1$ than 0 on indices $k+2, k+3$. Let $g_2 \in M_2$ be a flow that attains strictly more times 1 on $k, k+1$ than 0 on $k+2, k+3$, say $g_2(k+1) = 1$. By Lemma 4.16 we have $g_2(k+2), g_2(k+3) \neq 2$. If $g_2(k+2) = g_2(k+3) = 1$ we may exchange g_2 and g_1 on $k+1, k+2, k+3$, increasing k. By the choice of g_2 we must have $g_2(k) = 1$. Notice however that if $g_2(k+2) = 1$ (resp. $g_2(k+3) = 1$) we can exchange g_1 and g_2 on $k, k+1, k+2$ (resp. $k+3$), increasing k. Thus, $g_2(k+2) = g_2(k+3) = 0$, which contradicts the choice of g_2.

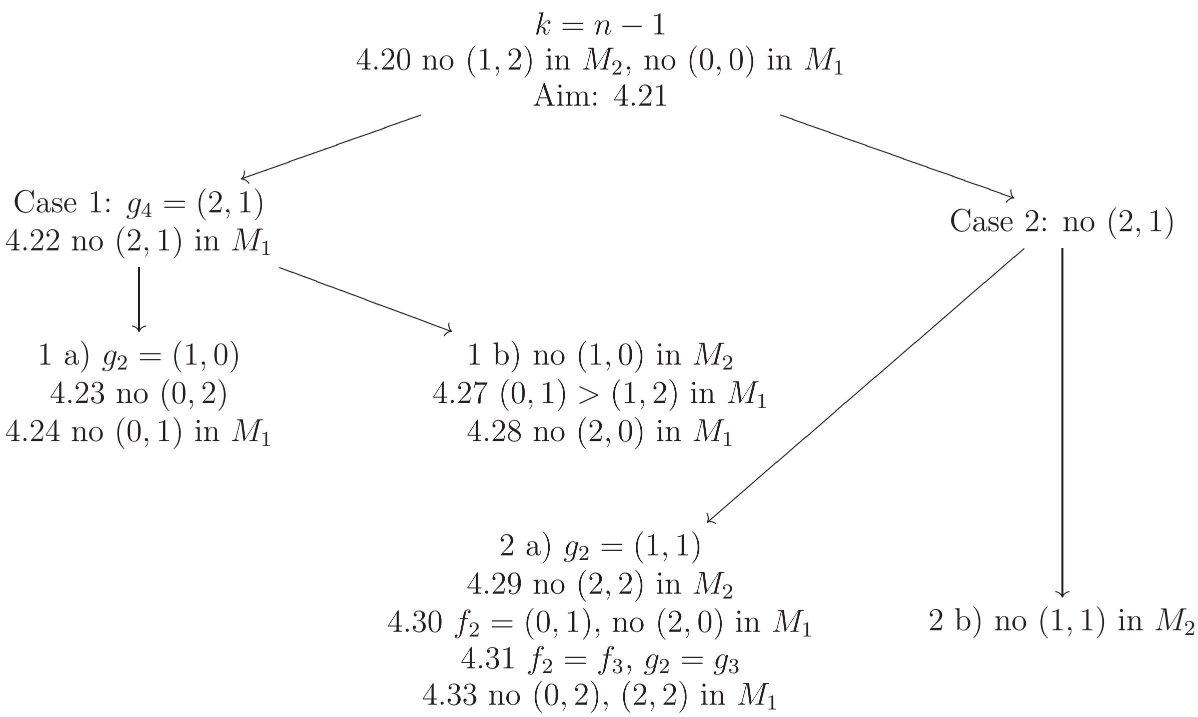
Case 2) There is no flow $f' \in M_1$ or $g' \in M_2$ such that:

(i) $f'(k) = f'(k+1) = 0$ or $f'(k+2) = f'(k+3) = 0$,

(ii) $g'(k) = g'(k+1) = 1$ or $g'(k+2) = g'(k+3) = 2$.

Hence, for any $f' \in M_1$ if $f'(k) = 0$ then $f'(k+1) = 1$. This contradicts the fact that for any $g' \in M_2$ if $g'(k+1) = 1$ then $g'(k) = 0$.

4.2. **Suppose $k = n - 1$.** As before we let $g_1 = \underline{0}$. We can also assume $f_1 = (0, \dots, 0, 1, 2)$. The diagram of the proof is as follows.



Definition 4.19 (type of a flow)**.** *We say that a flow f is of type (a, b) for $a, b \in \mathbb{Z}_3$ if $f(n-1) = a$ and $f(n) = b$.*

Lemma 4.20. *If there exists a flow*

(i) $g \in M_2$ of type $(1,2)$ or

(ii) $f \in M_1$ of type $(0,0)$,

then we can increase k. We thus assume that such flows do not exist.

Proof. Follows by obvious quadratic exchange. □

As M_1 and M_2 are compatible we can assume $f_2(n-1) = 0 \neq f_2(n)$, $f_3(n-1) \neq 0 = f_3(n)$, $g_2(n-1) = 1$, $g_2(n) \neq 2$, $g_3(n) = 2$, $g_3(n-1) \neq 1$. Our aim will be to prove the following proposition.

Proposition 4.21. *We can assume that for each flow $f \in M_1$ different from f_1 there exists at most one index $i < n-1$ such that $f(i) \neq f_2(i)$.*

We consider two cases.

Case 1) There exists a flow $g' \in M_1 \cup M_2$ of type $(2,1)$. In fact, by the action of $\mathcal{G}$ we can assume $g' \in M_2$. We let $g_4 = g'$.

Lemma 4.22. *We can assume there is no $f \in M_1$ of type $(2,1)$.*

Proof. In such a case we could exchange the flows so that $f_1(n-1) = g_1(n-1) = 2$ and $f_1(n) = g_1(n) = 1$ that would make the flows f_1 and g_1 equal. □

By Lemma 4.20 it is enough to consider two following subcases.

1 a) $g_2(n) = 0$

Lemma 4.23. *We can assume that there is no flow $g \in M_2$ of type $(0,2)$. Hence if $g(n) = 2$ then $g(n-1) = 2$.*

Proof. Assume such g exists. We can make an exhange between g_4, g, g_2 that on entries $n-1, n$ is as follows:

$$\begin{matrix} (2,1) & & (1,2) \\ (0,2) & = & (2,0) \\ (1,0) & & (0,1) \end{matrix} \cdot$$

This, by Lemma 4.20 increases k. The last statement follows from Lemma 4.20. □

Lemma 4.24. *We can assume that there is no flow $f \in M_1$ of type $(0,1)$. In particular, $f_2(n) = 2$.*

Proof. Suppose such f exists. First notice that we can assume that there is no $\tilde{f} \in M_1$ such that $\tilde{f}(n-1) = 2$ and $\tilde{f}(n) = 0$. Indeed, in such a case we could make an exchange among $f_1, f, \tilde{f}$ that on entries $n-1, n$ would be:

$$\begin{matrix} (1,2) & & (2,1) \\ (0,1) & = & (1,0) \\ (2,0) & & (0,2) \end{matrix} ,$$

that would allow to increase k by Lemma 4.22.

Hence, also by Lemma 4.22 we see that each $f_i \in M_1$ such that $f_i(n-1) = 2$ must satisfy $f_i(n) = 2$. Taking into account f_1 it follows that strictly more flows associate 2 to n than to $n-1$. This, looking at M_2, contradicts Lemma 4.23. □

Remark 4.25. *By Lemma 4.22 there must be at least as many flows of type $(2,0)$ as $(1,2)$ in M_1. Hence, we may assume that $f_3(n-1) = 2$ and f_2 and f_3 agree on indices $i < n-1$.*

We now prove Proposition 4.21 in Case 1 a).

Proof. Step 1: Flows of type $(1,2)$.

We will modify the flows of type $(1,2)$ differing from f_2 on at least 2 indices smaller than $n-1$. By Lemma 4.23 we know that there are at least as many flows that associate 2 to $n-1$ as those that associate 2 to n. By Lemma 4.22 there must be at least as many flows $\tilde{f} \in M_1$ such that $\tilde{f}(n-1) = 2$, $\tilde{f}(n) = 0$ as those $f \in M_1$ such that $f(n-1) = 1$, $f(n) = 2$. Hence, we can pair each f with $\tilde{f}$. If f differs from f_2 (hence also from f_3 and $\tilde{f}$) on some 2 indices smaller than $n-1$, then by Lemma 3.1 we can exchange f and $\tilde{f}$ on n, keeping $n-1$.

Step 2: Flows such that $f(n-1)=0$ *or* $f(n)=0$.

Here, the conclusion of the lemma follows from Lemma 3.1 by exchanging with f_2 or f_3. By previous lemmas the only cases left are flows of type $(1,1)$ or $(2,2)$.

Step 3: Flows of type $(1,1)$.

We can assume that each flow of type $(1,1)$ agrees with f_2 on all indices $i<n-1$. Indeed, otherwise, it it would differ on at least two indices, which we could exchange, obtaining at least two disagreements between f_2 and f_3. By Lemma 3.1 we could then obtain the flow of type $(0,0)$. Moreover, at least one flow $f_j \in M_1$ of type $(1,1)$ must exist as only such flows satisfy $f_j(n)=1$.

Step 4: Flows of type $(2,2)$.

If a flow of type $(2,2)$ differs from a flow of type $(1,1)$ (which is equivalent to differing from f_2) on at least two indices $i<n-1$ we would be able to make an exchange by Lemma 3.1 obtaining a flow of type $(2,1)$. This finishes the proof by Lemma 4.20. □

1 b) There is no flow $g \in M_2$ such that $g(n-1)=1$ and $g(n)=0$. In particular, $g_2(n)=1$. Notice that if $g \in M_2$ and $g(n-1)=1$, then $g(n)=1$.

Corollary 4.26. *Strictly more flows in* M_1 *associate* 1 *to* n *than to* $n-1$. □

Lemma 4.27. *There are strictly more flows* $f \in M_1$ *of type* $(0,1)$*, than those of type* $(1,2)$*. In particular, we can assume* $f_2(n)=1$.

Proof. Follows from Corollary 4.26 by Lemma 4.22. □

Lemma 4.28. *We can assume that there are no flows* $f \in M_1$ *of type* $(2,0)$*. In particular,* $f_3(n-1)=1$.

Proof. Indeed, in such a case we can exchange f, f_2, f_1 on indices $n-1, n$ as follows:

$$\begin{matrix}(2,0)\\(0,1)\\(1,2)\end{matrix} \quad = \quad \begin{matrix}(0,2)\\(1,0)\\(2,1)\end{matrix}$$

and conclude by Lemma 4.22. □

We now prove Proposition 4.21 in Case 1 b).

Proof. First notice that flows of type either $(0,1)$ or $(1,0)$ or $(2,2)$ must agree on indices smaller than $n-1$. Indeed, if such flows differ, they have to differ on at least two indices, that would allow to make an arbitrary exchange on indices $n-1, n$ by Lemma 3.1. There is always an exchange that allows to increase k.

We now consider flows $f \in M_1$, different from f_1, of type $(1,2)$. By Lemma 4.27 we can pair each such f with $\tilde{f}$, of type $(0,1)$. If $\tilde{f}$ and f differ on at least 2 indices smaller than $n-1$, by Lemma 3.1 we can make an exchange that on indices $n-1, n$ is as follows:

$$\begin{matrix}(0,1)\\(1,2)\end{matrix} \quad = \quad \begin{matrix}(1,1)\\(0,2)\end{matrix}.$$

The only flows left to consider are of type $(1,1)$ or $(0,2)$. Notice that there must exist a flow $f_j \in M_1$ of type $(2,2)$, as only such flow satisfies $f_j(n-1)=2$. If a flow of type $(1,1)$

exists and differs on at least two indices smaller than $n-1$ we can make an exchange by Lemma 3.1 with f_j:

$$\begin{matrix}(1,1) & & (1,2)\\ (2,2) & = & (2,1)\end{matrix},$$

that allows to increase k. If a flow $f' \in M_1$ of type $(0,2)$ exists and differs on at least two indices smaller than $n-1$ then we can find a subset $I \subset [0, n-2]$ such that $\sum_{i\in I} f'(i) = \sum_{i\in I} f_2(i)+1$. We can then make an exchange among f', f_3, f_1 that on indices $I, n-1, n$ is as follows:

$$\begin{matrix}(a+1,0,2) & & (a,1,2)\\ (a,1,0) & = & (a+1,1,2)\\ (\underline{0},1,2) & & (\underline{0},0,0)\end{matrix},$$

where we represent all values of f_3 on I by a. □

Case 2) There is no flow f among $M_1 \cup M_2$ such that $f(n-1) = 2$ and $f(n) = 1$. We consider two subcases.

Case 2 a) There exists a flow $g \in M_2$ such that $g(n-1) = g(n) = 1$. In this case we let $g_2 = g$.

Lemma 4.29. *If there is a flow $g \in M_2$ of type $(2,2)$ then we can increase k. In particular we may assume $g_3(n-1) = 0$.*

Proof. In such a case we can apply the relation among g_1, g_2, g that on indices $n-1, n$ is of the following form:

$$\begin{matrix}(0,0) & & (1,2)\\ (1,1) & = & (2,0)\\ (2,2) & & (0,1)\end{matrix}.$$

□

Lemma 4.30. *We may assume that $f_2(n) = 1$. Moreover, if there is a flow $f \in M_1$ of type $(2,0)$ then we can make a reduction. In particular, we may assume $f_3(n-1) = 1$.*

Proof. First let us note that the first sentence implies the second. Indeed, we can make an exchange among f_1, f, f_2 that on indices $n-1, n$ would be:

$$\begin{matrix}(1,2) & & (0,0)\\ (2,0) & = & (1,1)\\ (0,1) & & (2,2)\end{matrix}.$$

To prove the first sentence assume the contrary that for any $f' \in M_1$ if $f'(n-1) = 0$ then $f'(n) = 2$. It follows that strictly more flows associate 2 to n than 0 to $n-1$. This contradicts Lemma 4.29. □

Lemma 4.31. *We can assume that:*

(i) the flows f_2 and f_3 agree on all indices smaller than $n-1$ and
(ii) the flows g_2 and g_3 agree on all indices smaller than $n-1$.

Proof. Each pair, if it differs, it must differ on at least 2 indices and the conclusion follows from Lemma 3.1. □

Lemma 4.32. *We can assume that each flow $f \in M_1$ different from f_1 either:*

(i) differs from f_2 *only on one index smaller than* $n-1$, *or*
(ii) $f(n-1) = f(n) = 1$ *and* f *differs from* f_2 *on exactly two indices* $i, j < n-1$ *for which* $f(i) = f_2(i) + 1$, $f(j) = f_2(j) + 1$

Proof. We only have to consider flows of types: $(0,1)$, $(0,2)$, $(1,0)$, $(1,1)$, $(1,2)$, $(2,2)$. From Lemma 4.31 we obtain that $(0,1)$, $(1,0)$ and $(2,2)$ agree on all entries smaller than $n-1$. If a $(0,2)$ flow differs on two indices, we can increase k by Lemma 3.1. If any flow f differs on at least 3 indices we can exchange f, f_2, f_3 obtaining a flow that assigns 0 both to $n-1$ and n. Hence, to prove the Lemma, we only need to consider flows f of type $(1,2)$ for which there are two indices $i', j' < n-1$ such that $f(i') = f_2(i') + 2$, $f(j') = f_2(j') + 2$.

Flows of type $(1,2)$ can be paired with $(0,1)$ flows (if there are not enough $(0,1)$ flows we can apply Lemma 4.30) and in each pair we can apply the relation:

$$\begin{matrix}(a,0,1)\\(a+2,1,2)\end{matrix} \quad = \quad \begin{matrix}(a+2,1,1)\\(a,0,2)\end{matrix},$$

where $a = f_2(i')$. □

Lemma 4.33. *Either all flows in* M_1 *apart from* f_1 *differ from* f_2 *on at most one index smaller than* $n-1$ *or we can assume there are no flows* $f \in M_1$ *of type* $(0,2)$ *or* $(2,2)$.

Proof. Suppose there exists a flow f described in point 2) of Lemma 4.32. If a flow of type $(0,2)$ exists we can exchange it with f on last two entries obtaining a contradiction with Lemma 4.32.

If a flow of type $(2,2)$ exists we can make an exchange obtaining a flow of type $(2,1)$, hence reduce to Case 1). □

To finish the proof of Proposition 4.21 we have to prove that there exists a flow in M_1 of type $(0,2)$ or $(2,2)$. Suppose this is not the case - we will reach a contradiction. All flows in M_1 are of one of the types $(1,2)$, $(0,1)$, $(1,0)$, $(1,1)$. It follows that the flows in M_2 can be only of types $(0,0)$, $(1,1)$, $(0,2)$, $(1,0)$, $(0,1)$.

Choose an index $i < n-1$ such that $f_2(i) \neq g_2(i)$. Suppose there are x flows of type $(1,2)$ in M_1. Then there are also x flows of type $(0,2)$ among M_2. Let there be y flows of type $(0,1)$ and z of type $(0,0)$ in M_2. Then there are $x+y+z$ flows of type $(0,1)$ in M_1. Let w be the number of flows of type $(1,1)$ in M_1. Then there are $x+z+w$ flows of type $(1,1)$ in M_2. Suppose there are q flows of type $(1,0)$ in M_2. Then there are $z+q$ flows of type $(1,0)$ in M_1. Hence, on index i, $f_2(i)$ appears at least $x+z+y+z+q$ times and $g_2(i)$ appears at least $x+z+w+x$ times. However, the sum of these two numbers $3x+3z+y+q+w$ is larger than the cardinality of the multisets $2z+2x+w+q+y$, which gives the contradiction.

Case 2 b) There is no flow $g \in M_2$ such that $g(n-1) = g(n) = 1$. By the action of $\mathcal{G}$ we can reduce to Case 2 a) also when:

(i) there is a flow of type $(0,1)$ in M_1 (by the nontrivial automorphism of $\mathbb{Z}_3$),
(ii) there is a flow of type $(2,0)$ in M_1 (by the transposition of $n-1$ and n).

Recall that we also know that there are no flows of type $(0,0)$ or $(2,1)$ in M_1. By the case assumption we know that in M_2 there are no flows of type $(1,1)$, $(1,2)$. Hence, strictly more flows in M_2 associate 0 to n than 1 to $n-1$. This contradicts the fact that there are no flows of type $(2,0)$ and $(0,0)$ in M_1.

This finishes the proof of Proposition 4.21.

Among all the multisets that can be reached from $M_2 \setminus g_1$ by exchanging at most three flows, let $\tilde{M}_2$ be one (possibly out of many) that minimizes the number s of indices smaller than $n-1$ on which a flow from $\tilde{M}_2$ can differ from f_2. Further, it also minimizes the number of flows differing on exactly s indices, and further on $s-1$ indices. First note that $s \leq 3$. Indeed, if there is a flow $g \in \tilde{M}_2$ differing on 4 indices, by compatibility we can find a flow $\tilde{g} \in \tilde{M}_2$ that equals f_2 on $[n-2]$ and we can make an exchange on 2 or 3 indices.

Suppose $s = 3$. By compatibility we can find a flow $\tilde{g} \in \tilde{M}_2$ that equals f_2 on $[n-2]$ (there exist at least three such flows). Let $\tilde{g}$ be of type (a, b). Without loss of generality we can assume that $g \in \tilde{M}_2$ and $g(l) = f_2(l) + 1$ for $l = 1, 2, 3$. There can be no flows in $\tilde{M}_2$ that attain $f_2(i) + 2$ at index i for any $i < n-1$, as we would be able to make an exchange with g and $\tilde{g}$. By the definition of $\tilde{M}_2$ all flows in that multiset that differ from f_2 on 3 indices in $[n-2]$ must also be of type (a, b). So must all the flows that agree with f_2. Further, flows that differ on 1 or 2 indices must either have a on $n-1$ or b on n. By compatibility there must exist a flow in M_1 of type (a, b). We may assume that f_2 is of type (a, b) and equals $\tilde{g}$.

Suppose $s = 2$. Without loss of generality there are at least as many flows in $\tilde{M}_2$ that differ from f_2 on indices $1, 2$ as on indices $4, 5$. We pair each flow that differs on $4, 5$ with a flow that differs on $1, 2$. By Lemma 3.1 we can make an exchange in each pair, in such a way that none of the flows differs both on 4 and 5. Then for $i, j = 4, 5$ we proceed exactly as in Lemma 4.15 and the paragraph after it.

If $s = 1$ or $s = 0$ we may proceed as above, choosing any $i, j \leq n-2$. This finishes the proof of the main theorem.

References

[Alo99] Noga Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29, Recent trends in combinatorics (Mátraháza, 1995). MR 1684621 (2000b:05001)

[BBKM13] Weronika Buczyńska, Jarosław Buczyński, Kaie Kubjas, and Mateusz Michałek, *On the graph labellings arising from phylogenetics*, Cent. Eur. J. Math. **11** (2013), no. 9, 1577–1592. MR 3071924

[Bru13] Winfried Bruns, *The quest for counterexamples in toric geometry*, Commutative algebra and algebraic geometry (CAAG-2010), Ramanujan Math. Soc. Lect. Notes Ser., vol. 17, Ramanujan Math. Soc., Mysore, 2013, pp. 45–61. MR 3155951

[BTRS01] Winfried Bruns, Richard Sieg Tim Römer, and Christof Söger, *Normaliz*, http://www.home.uni-osnabrueck.de/wbruns/normaliz/ (2001).

[BW07] Weronika Buczyńska and Jarosław A. Wiśniewski, *On geometry of binary symmetric models of phylogenetic trees*, J. Eur. Math. Soc. **9(3)** (2007), 609–635.

[CFSM14] Marta Casanellas, Jesús Fernández-Sánchez, and Mateusz Michałek, *Low degree equations for phylogenetic group-based models*, Collectanea Mathematica (2014), 1–23.

[CLS11] David A. Cox, John B. Little, and Henry K. Schenck, *Toric varieties*, Graduate Studies in Mathematics, vol. 124, American Mathematical Society, Providence, RI, 2011. MR 2810322 (2012g:14094)

[CP07] J. Chifman and S. Petrović, *Toric ideals of phylogenetic invariants for the general group-based model on claw trees $k_{1,n}$*, Proceedings of the 2nd international conference on Algebraic biology (2007), 307–321.

[DB16] Maria Donten-Bury, *Phylogenetic invariants for $\mathbb{Z}_3$ scheme-theoretically*, Annals of Combinatorics (2016), 1–20.

[DBM12] Maria Donten-Bury and Mateusz Michałek, *Phylogenetic invariants for group-based models*, Journal of Algebraic Statistics **3** (2012), no. 1, 44–63.

[DE15] Jan Draisma and Rob H. Eggermont, *Finiteness results for Abelian tree models*, J. Eur. Math. Soc. (JEMS) **17** (2015), no. 4, 711–738. MR 3336833

[DK09] Jan Draisma and Jochen Kuttler, *On the ideals of equivariant tree models*, Mathematische Annalen **344(3)** (2009), 619–644.

[DK14] Jan Draisma and Jochen Kuttler, *Bounded-rank tensors are defined in bounded degree*, Duke Math. J. **163** (2014), no. 1, 35–63. MR 3161311

[ERSS04] N. Eriksson, K. Ranestad, B. Sturmfels, and S. Sullivant, *Phylogenetic algebraic geometry*, Projective Varieties with Unexpected Properties; Siena, Italy (2004), 237–256.

[Ful93] William Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies, vol. 131, Princeton University Press, Princeton, NJ, 1993, The William H. Roever Lectures in Geometry.

[Kub12] Kaie Kubjas, *Hilbert polynomial of the kimura 3-parameter model*, Journal of Algebraic Statistics **3** (2012), no. 1, 64–69.

[Las10] Michał Lasoń, *A generalization of combinatorial Nullstellensatz*, Electron. J. Combin. **17** (2010), no. 1, Note 32, 6. MR 2729390 (2012c:05352)

[LM14] Michał Lasoń and Mateusz Michałek, *On the toric ideal of a matroid*, Advances in Mathematics **259** (2014), 1–12.

[Man09] C. Manon, *The algebra of Conformal Blocks*, arXiv:0910.0577 (2009).

[Man12] Christopher Manon, *Coordinate rings for the moduli stack of sl2(c) quasi-parabolic principal bundles on a curve and toric fiber products*, Journal of Algebra **365** (2012), 163–183.

[Man13] ———, *The algebra of* $\mathbf{SL}_3$ *conformal blocks*, Transformation Groups **18** (2013), no. 4, 1165–1187.

[Mic10] Mateusz Michałek, *A short proof of combinatorial Nullstellensatz*, Amer. Math. Monthly **117** (2010), no. 9, 821–823. MR 2760383

[Mic11] ———, *Geometry of phylogenetic group-based models*, Journal of Algebra **339** (2011), no. 1, 339–356.

[Mic13] ———, *Constructive degree bounds for group-based models*, Journal of Combinatorial Theory, Series A **120** (2013), no. 7, 1672–1694.

[Mic14] ———, *Toric geometry of the 3-kimura model for any tree*, Advances in Geometry **14** (2014), no. 1, 11–30.

[Mic15] ———, *Toric varieties in phylogenetics*, Dissertationes Mathematicae **511** (2015), 1–86.

[MRV14] Marie Mauhar, Joseph Rusinko, and Zoe Vernon, *H-representation of the kimura-3 polytope*, arXiv preprint arXiv:1409.4130 (2014).

[PS05] Lior Pachter and Bernd Sturmfels (eds.), *Algebraic statistics for computational biology*, Cambridge University Press, New York, 2005.

[RH12] Joseph P Rusinko and Brian Hipp, *Invariant based quartet puzzling.*, Algorithms for Molecular Biology **7** (2012), no. 1, 35.

[SS05] Bernd Sturmfels and Seth Sullivant, *Toric ideals of phylogenetic invariants*, J. Comput. Biology **12** (2005), 204–228.

[Stu96] Bernd Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, 1996.

[Sul07] Seth Sullivant, *Toric fiber products*, Journal of Algebra **316** (2007), no. 2, 560 – 577, Computational Algebra.

[SX10] Bernd Sturmfels and Zhiqiang Xu, *Sagbi bases of Cox-Nagata rings*, Journal of the European Mathematical Society **12** (2010), 429–459.

[tt] 4ti2 team, *4ti2—a software package for algebraic, geometric and combinatorial problems on linear spaces*, www.4ti2.de.

Mateusz Michałek, Polish Academy of Sciences, Warsaw, Poland, `wajcha2@poczta.onet.pl`